Output Encoding

Paul Mooney
Chief Software Architect, Microsoft MVP

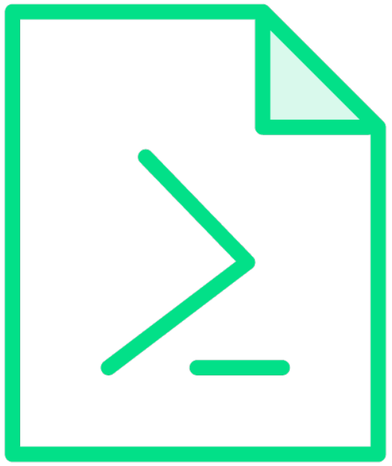
@daishisystems | www.insidethecpu.com

Overview

Output Encoding in a Nutshell

- OWASP Top 10 #3 – Injection
- Multiple data sources
- Data is output to media
- Malicious code injection
- Input field or URL parameter
- Strong output encoding policies

Cross-Site Scripting (XSS)



What is Cross-Site Scripting?

- Inject malicious code
- Steal sensitive information
- Perform actions on behalf of user

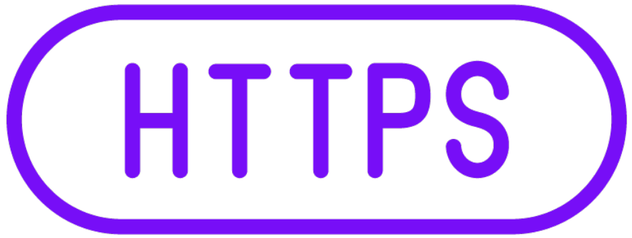
Types of Cross-Site Scripting Attack

Reflected XSS

Stored XSS

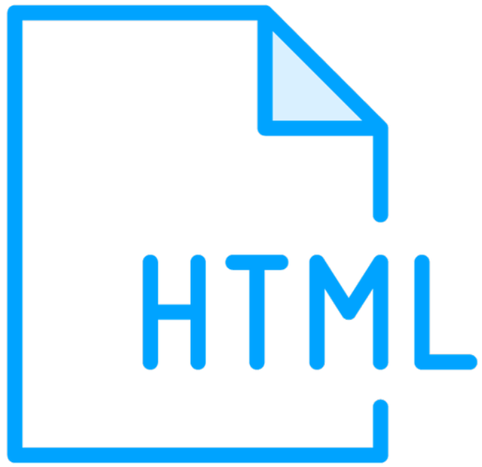
Document Object Model-based XSS

Types of XSS Attack



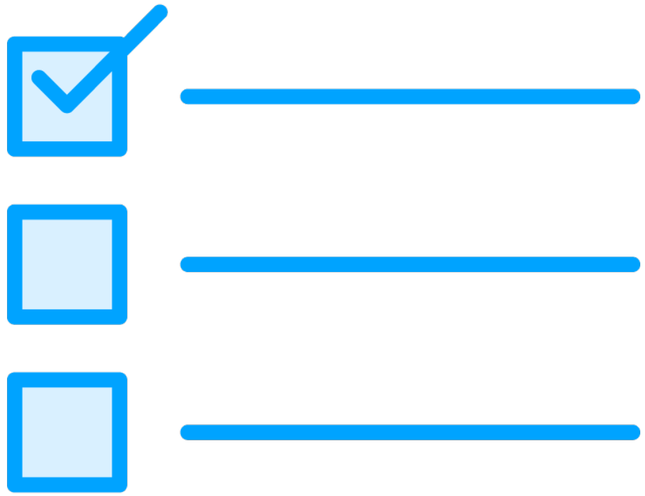
Modifying the HTTP Content-Type Header

- Content-Type Sniffing
- MIME Sniffing
- Bypass output encoding
- Restrict type of content
- Modify the Content-Type header
- Inject code into a file



Manipulating HTML Tags

- Exploiting form input field
- HTML entity encoding
- JavaScript escaping
- Content Security Policy (CSP)
- Automatically encode input
- 3rd party libraries



Remember ...

- Validate input
- Encode input
- Strict security policies

Demo

Preventing XSS Attacks with Output Encoding

- Simulate an XSS attack
- Apply HTML template
- Prevent XSS attacks by encoding output

Demo

Preventing SQL Injection Attacks

- Inject SQL code into user interface
- Manipulate application database
- Unauthorized access
- Data modification
- Safely transforms characters
- Our demo app ...

Summary

Output Encoding

- Cross-Site Scripting (XSS)
- SQL Injection
- Properly sanitize user data
- Escape special characters
- Appropriate encoding scheme
- Parameterize database queries